# LEGAL ANALYSIS OF LAW ENFORCEMENT IN THE FRAUD CASE AT BANK JAGO

**Raihan Muhammad[1], Amirul Makhfud[2], Bintang Rafli Ananta[3], Muhammad Rizqi Robbani[4], Fauzuld Nur Arsy[5]**

[1-5)]Legal Studies, Faculty of Law, Universitas Negeri Semarang
[1*]rainesia15@gmail.com, [2]amirulmakhfud608@gmail.com,[3]raflianta3598@students.unnes.ac.id
[4]rizqirobbani30@students.unnes.ac.id, [5]arsyfauzuldnur@gmail.com

***Abstract***

*This research analyzes a fraud case at Bank Jago involving the embezzlement of customer funds worth Rp1.3 billion by a former bank employee in 2023. This case is of concern because it reveals weaknesses in the internal monitoring system and the risk of abuse of authority. Using a normative legal approach and qualitative descriptive methods, this research examines the chronology of events, the perpetrator's modus operandi, and the effectiveness of applicable regulations. Research data was obtained from secondary sources such as official reports, statutory regulations, internal bank policies, and scientific articles. The research results show that weak internal supervision and unauthorized access are the main causes of fraud. The perpetrators used their authority to illegally unblock customer accounts and transfer funds to their personal accounts, which violates the ITE Law, Fund Transfer and TPPU. This research highlights the importance of applying advanced technology such as artificial intelligence and big data analytics to detect potential fraud, synergy between banking institutions and law enforcement officials, as well as employee training to build an antifraud culture. With these recommendations, it is hoped that research can contribute to improving the integrity and security of the banking sector in Indonesia.*

***Keywords:*** *Legal Analysis, Banking Fraud, Law Enforcement*

## INTRODUCTION

Fraud in the banking world is a serious threat that can harm the bank, customers, and the wider community. This fraud is often closely related to weak internal banking supervision and control systems. In this case, the rapid development of information technology in the banking sector provides new opportunities for criminals to exploit security gaps, thereby creating new challenges in efforts to prevent and overcome fraud. The theft of Rp1.3 billion in funds committed by former Bank Jago employees from 18 March to 31 October 2023 is a clear example that shows the complexity of this problem. The perpetrator, a contact center specialist, used his authority to unblock accounts previously frozen by law enforcement officials (Oktafian, 2024). This action revealed weaknesses in the banking sector's internal supervision and risk management systems.

Previous studies show that banking fraud can be minimized through strengthening anti-fraud strategies and implementing effective early detection technology. According to research by Kristianti, Kuntadi, & Pramukty (2023) and Lestari & Geraldina (2023), the success of implementing an effective internal control system is very dependent on the level of compliance and integrity of employees in all lines of banking operations. Apart from that, Arifin (2018) highlighted the importance of synergy between banking institutions and law enforcement officials in handling fraud cases to ensure a deterrent effect for perpetrators and improve the existing system.

The challenges in overcoming banking fraud are increasingly complex with the development of digital technology, which allows criminals to exploit loopholes in existing systems. Banks that adopt advanced technologies, such as digital banking systems and online transactions, often face new risks related to data security and transaction protection. This phenomenon demands a paradigm shift in the risk control approach, where traditional methods that rely more on manual supervision are becoming less effective. Therefore, it is essential to encourage the implementation of more sophisticated security systems, including artificial intelligence (AI) and big data analytics, to detect

fraud patterns that are not detected by conventional systems. In dealing with this situation, increasing human resource capacity in the banking sector is also an aspect that is no less important. Continuous training and raising awareness of potential fraud risks are the keys to creating an anti-fraud culture in every line of banking. This aligns with research results showing that fraud often occurs due to negligence or deliberate actions of employees with excellent access to the banking system.

On the other hand, strong regulations and consistent law enforcement are also essential parts of fraud prevention efforts. As suggested by Arifin (2018), closer cooperation between the banking sector and law enforcement officials will strengthen mechanisms for detecting and taking action against fraud cases. The government and banking authorities need to continue to evaluate existing regulations and ensure that sanctions against fraud perpetrators are sufficient to provide a deterrent effect and prevent similar incidents from recurring. Based on this background, this article aims to analyze the fraud case at Bank Jago by reviewing the chronology of perpetrators and banking institutions, as well as legal facts and legal responsibility. This research also recommends increasing the effectiveness of law enforcement and fraud mitigation strategies in the banking sector. Thus, it is hoped that this article can contribute to developing fraud prevention discourse and practice in Indonesia's banking industry.

## METHOD

This research method uses a normative legal analysis approach to examine legal aspects related to law enforcement in fraud cases at Bank Jago. The approach used is descriptive-qualitative, where researchers describe and analyze legal phenomena that occur in the context of fraud cases in detail and in-depth (Efendi & Rijadi, 2022). The first step in this research was a review of documents and literature, including the laws and regulations governing fraud prevention in the banking world, Bank Jago's internal policies, and relevant previous studies. This study aims to understand the legal basis for dealing with fraud cases and the regulations governing supervision and control in the banking sector.

This research will analyze cases of fraud that occurred at Bank Jago. Researchers will collect data regarding the chronology of events, the modus operandi used by the perpetrators, and internal bank policies considered ineffective in preventing fraud. In this case, researchers will analyze the factors that allow fraud to occur and evaluate the existing monitoring system. The researcher will utilize secondary data from various sources, including official reports, company documents, and relevant scientific articles. This data will provide a clear picture of Bank Jago's internal policies and the legal steps that have been taken to handle these fraud cases. Researchers will also analyze various sources containing perspectives from legal experts, regulators, and banking practitioners who focus on preventing and overcoming fraud.

This research will conduct a legal analysis to evaluate legal liability for fraud perpetrators, both from the criminal aspect and administrative sanctions against banks, and assess the extent to which existing regulations effectively tackle this crime. Based on the findings obtained, this research will also provide policy recommendations to strengthen the internal supervision system in the banking sector and increase synergy between banking institutions and law enforcement officials in preventing fraud. Researchers will also propose more effective regulatory improvements to prevent the recurrence of similar cases, increase law enforcement, and improve the internal control system at Bank Jago.

This research employs the normative legal method, focusing on written legal sources such as laws, regulations, court decisions, contracts, and legal theories, primarily analyzing legal documents. Library research relies on secondary data from extensive reviews of official reports, company policies, scholarly articles, and previous studies (Muhammad, 2024). The statute approach examines laws and regulations pertinent to fraud cases at Bank Jago, including frameworks for fraud prevention, internal controls, and sanctions. This qualitative study interprets verbal expressions and written materials to assess legal measures, analyze the modus operandi of fraud, and identify inadequacies in Bank Jago’s internal policies.

The research aims to evaluate perpetrators' legal liability from criminal and administrative perspectives while also assessing the effectiveness of existing regulations. By engaging with statutory frameworks and expert insights, the study provides policy recommendations for improving internal supervision systems, fostering stronger collaboration between banking institutions and law

enforcement, and enhancing regulatory measures to prevent future fraud cases. This analysis contributes to a deeper understanding of law enforcement's role in addressing fraud and strengthening the integrity of the banking sector.

## RESULTS AND DISCUSSION

### The Case of Bank Jago Customer Account Breach by a Former Employee

The case of customer fund embezzlement by a former employee of Bank Jago, IA, provides a clear picture of significant legal violations in the banking sector, regarding the chronology of events and the revealed legal facts. Chronologically, this unlawful act began with IA's misuse of authority as a contact center specialist from March to October 2023. IA illegally unblocked 112 customer accounts that had previously been frozen at the request of Law Enforcement Agencies (LEAs) due to indications of criminal activity. Using her system access, IA transferred customer funds amounting to IDR 1.397 billion into a collection account she had prepared for personal purposes, including paying debts and funding her family vacations (Fadilah 2024).

This criminal act was eventually uncovered when Bank Jago's fraud detection system recorded suspicious activity on its system. Through an internal investigation, the bank discovered that the suspicious activities originated from unauthorized access by IA. Realizing the severity of the violation, Bank Jago immediately reported these findings to the police. On July 4, 2023, IA was arrested in East Ciputat, South Tangerang, at around 00:50 WIB (Wicaksono 2024). The arrest was accompanied by confiscating evidence, including two cellphones belonging to the perpetrator and system access logs showing the account unblocking activities. Investigations revealed that IA's actions spanned approximately seven months, involving a series of unauthorized approvals for 112 frozen accounts.

This case garnered significant attention because it highlighted weaknesses in the bank's internal supervision and raised concerns about customer data and fund security. Bank Jago took proactive measures to ensure that no customers were financially harmed and committed to improving system security to prevent similar incidents from happening again. On the other hand, the legal process against IA continues with relevant provisions from the Electronic Information and Transactions Law (EIT), the Fund Transfer Law, and the Prevention and Eradication of Money Laundering Law.

Bank Jago's success in detecting suspicious activities highlights the importance of implementing an effective fraud detection system. This system allowed internal investigations to be conducted quickly, ultimately leading to the perpetrator's arrest on July 4, 2023, in East Ciputat, South Tangerang. This chronology illustrates the importance of a robust internal supervision mechanism in maintaining the integrity of the banking system.

Furthermore, a closer examination of the case of fund embezzlement by former Bank Jago employee IA reveals several important legal facts that serve as the basis for law enforcement. The first fact is the unauthorized access to Bank Jago's system. IA, as a contact center specialist, exploited her authority to unlawfully unblock 112 customer accounts. These accounts had previously been frozen at the request of LEAs due to suspected involvement in criminal activity. This unauthorized access, without official authorization from investigators, constitutes a violation of Article 30 paragraph (1) jo Article 46 paragraph (1) and Article 32 paragraph (1) jo Article 48 paragraph (1) of Law No. 19 of 2016 on Electronic Information and Transactions (EIT) (Djailani 2024).

On the other hand, Bank Jago managed to demonstrate its accountability as a financial institution by ensuring that no customers were financially harmed. The bank also showed its commitment to improving security systems and enhancing risk mitigation measures to prevent similar cases in the future. This step is important not only to maintain customer trust but also to uphold the bank's reputation within the banking industry.

The second fact is the transfer of funds amounting to IDR 1.397 billion from frozen customer accounts to the collection account prepared by the perpetrator. This transfer violated the fund transfer mechanism stipulated in Article 81 of Law No. 3 of 2011 on Fund Transfers. This action also fulfilled the elements of money laundering as regulated in Articles 3, 4, and 5 of Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes (Wanda 2020:5). IA used the funds for

personal needs, including paying debts and covering recreational expenses, which reinforced economic motives as the driving factor behind her actions.

Additionally, other legal facts indicate that Bank Jago had implemented risk mitigation measures through an early fraud detection system. This was proven by the bank's success in detecting suspicious activities conducted by IA, enabling swift internal investigations before reporting the matter to law enforcement. This step demonstrates good risk management implementation in line with anti-fraud principles as regulated in banking legislation.

The final legal fact is Bank Jago's legal responsibility towards its customers. Bank Jago ensured that no customers were financially harmed as a result of this action by guaranteeing the return of the embezzled funds. Furthermore, the bank committed to improving system security and continuing cooperation with law enforcement to ensure the perpetrator is prosecuted in accordance with the applicable laws. These legal facts not only strengthen the charges against the perpetrator but also serve as an important reflection for the banking world in reinforcing public trust in the financial system.

This case serves as an important reflection on the necessity of integrity in managing banking systems. Moreover, the application of firm legal measures against the perpetrator sends a message that crimes in the banking sector will be dealt with according to the prevailing laws. This discussion emphasizes the need for strengthening regulations and oversight in the financial sector to safeguard the security, trust, and sustainability of the banking industry.

The review of this problem cannot actually stop if it is limited to the issue of "frauding" and "violation of the provisions of the Banking Law". Remembering, this violation actually intersects with illegal access to personal data. Therefore, the author will also review this issue with the provisions contained in Law Number 27 of 2022 concerning Personal Data Protection or hereinafter referred to as the PDP Law. Although the intersection is on a thin line, when we refer to the opinions of scholars, such as Mahira, et all in Suari and I Made Sarjana (2023:135) it is stated that "Personal Data" essentially refers to various information in various forms that can identify individuals directly or indirectly, which through this sense actually has a relationship with the provisions in Article 4 paragraph (2) of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), where "financial data" can be identified as Specific Personal Data. Therefore, the act of "illegal access" to the blocked account as the context in this case, can actually be reviewed through the provisions of the PDP Law. In this context, account numbers and related activities that are illegally accessed by Bank Jago employees can be classified as personal data that must be protected. This strengthens the argument that breaches of financial data also include violations of legitimate personal data protection principles.

It should be agreed from the outset that the Right to Privacy for personal data was born with the aim of protecting every human right and individual dignity, as well as to ensure that personal data is used ethically for all parties, including the government, the private sector, and other entities that manage personal data. (Latumahina) Thus, the victim of illegal access in this case can be said to be a "subject of personal data" as defined in Article 1 paragraph (6) of the PDP Law, namely "an individual to whom personal data is attached." Although the illegally accessed customer account is indicated to be connected to a criminal act, the rights of the personal data subject remain inherent as long as there is no court ruling that legally revokes it. Therefore, victims of illegal access have the right to: First, obtain clear information regarding the identity of the party accessing their personal data; Second, Understand the basis of legal interests and the purpose of accessing personal data as stipulated in Article 7 of the PDP Law; Third, demanding accountability of personal data managers for violations that occur. Furthermore, Article 12 of the PDP Law stipulates that personal data subjects have the right to sue and receive compensation for violations in the processing of personal data. In the case of Bank Jago, victims of illegal access have a legal basis to demand these rights from the responsible party.

Departing from this fact, Bank Jago can thus be said to be the Controller and Processor of Personal Data. As for the Personal Data Controller, it has been regulated in Article 19 of the PDP Law, which states that the personal data controller includes every person, legal entity, and international organization responsible for the processing of personal data. In this case, Bank Jago has a role as a personal data controller, which is required to comply with the provisions in Article 20 paragraph (2), including: First, Obtaining valid consent from the personal data subject; Second,

complying with personal data protection obligations; Third, Fulfilling legal obligations related to data processing; Fourth. Protect the vital interests of the subject of personal data; and Fifth, Safeguarding legitimate interests in accordance with laws and regulations. However, the actions taken by Bank Jago employees show a violation of these provisions. In fact, every processing of personal data must meet the elements of consent of the personal data subject as stipulated in Article 21 paragraph (2). Illegal access by perpetrators proves that the mechanism for controlling and processing personal data at Bank Jago has not fully met the protection standards regulated in the PDP Law.

It should be emphasized once again that Bank Jago, as a data controller, has an obligation to ensure the security of customers' personal data and ensure that there is no misuse of access by internal parties. Violations by employees reflect weaknesses in internal supervision that can result in administrative sanctions and lawsuits by victims in accordance with Articles 57 to 58 of the PDP Law. Meanwhile, victims of personal data breaches have the right to recovery, both in the form of material and non-material compensation. Bank Jago is obliged to ensure that the recovery process runs transparently and fairly to restore public confidence in the banking system.

Actually, the provisions in the PDP Law have regulated the threat of sanctions for personal data violations, both administrative sanctions and criminal sanctions. In the case of administrative sanctions, it may be in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data; and/or administrative fines. Talking about the administrative fines imposed, it actually refers to Article 57 paragraph (3) which states that the administrative fine is a maximum of 2 percent of the annual income or annual revenue for the violation variable. In addition to administrative sanctions, criminal provisions may also be imposed on those who violate the provisions on personal data protection as stipulated in Article 67 paragraph (1) which states that "Any Person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or others that may result in losses to the Personal Data Subject" will be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah) as stipulated in Article 5 paragraph (1). Then in Article 65 paragraph (3) it is also stated that "Every person who deliberately and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 Paragraph 3 shall be sentenced to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah)".

Although through these various provisions, Bank Jago as a personal data processor has clearly violated the provisions of the PDP Law, but it should be noted that the PDP Law came into effect in Indonesia on October 17, 2024 even though it had been passed two years earlier, on October 17, 2022 to be precise. As for the a quo case revealed in July 2024, if it refers to the principle of "geen straf zonder schuld" or the principle of no crime without fault, then Bank Jago, along with the perpetrators, cannot be subject to violations of the provisions of the PDP Law. Therefore, the ideal punishment is only imposed for violations of the provisions of the ITE Law and the Banking Law.

**Legal Responsibility for Bank Jago Customer Account Breach Case by Former Employee**

Bank Jago's fraud case, involving its former employee IA, is one of the cases that caught the public's attention as it not only reflects a serious violation of the law, but also exposes loopholes in internal controls in the banking sector. The crime involved the embezzlement of Rp1.397 billion in customer funds by IA, a contact center specialist, during the period March to October 2023. Utilizing access to bank systems that should have been used for professional purposes, IA unblocked 112 customer accounts that were previously frozen at the request of law enforcement officials due to indications of criminal activity. This illegal access was used by IA to transfer funds to his personal accounts, which were then used for various personal needs such as paying debts and financing family vacations.

The crime was eventually uncovered thanks to the fraud detection system implemented by Bank Jago. The system noted suspicious activity, which was then followed up by an internal investigation by the bank. The findings of the investigation revealed that IA had made repeated unauthorized access to the bank's systems, as well as abused his authority to commit criminal acts. Recognizing the seriousness of this breach, Bank Jago immediately reported the case to the police.

On July 4, 2023, IA was arrested in East Ciputat, South Tangerang, along with evidence in the form of two cellphones and system access logs showing details of his illegal activities.

From a legal perspective, the actions committed by IA can be categorized as serious violations involving a number of laws and regulations that apply in Indonesia. In the context of the Electronic Information and Transaction Law (UU ITE), IA violated Article 30 paragraph (1) jo Article 46 paragraph (1), which stipulates that unauthorized access to electronic systems is a criminal offense. As a contact center specialist, IA abused his authority to unblock customer accounts without permission, which clearly violates the legal provisions regarding system access that may only be done by authorized parties. In addition, IA was also proven to have violated Article 32 paragraph (1) jo Article 48 paragraph (1) of the ITE Law related to electronic data manipulation, because he changed the blocking status of customer accounts and transferred funds without official approval. This manipulation not only violates customer privacy but also creates material losses.

Furthermore, IA's actions violate the fund transfer mechanism stipulated in Article 81 of Law No. 3/2011 on Fund Transfers. In this regulation, it is explained that every fund transfer must be carried out in accordance with established procedures to ensure the security and legality of the transaction. However, IA transferred funds from the blocked customer account to his personal account without fulfilling these procedures, which is a serious violation of the applicable fund transfer system. This crime also fulfills the elements of the crime of money laundering as stipulated in Articles 3, 4, and 5 of Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (TPPU). The Rp1.397 billion that IA embezzled was used for personal needs such as paying debts and family vacations. The use of these funds indicates an intention to disguise the origin of the illegal funds, which is one of the main elements in the crime of money laundering. The IA's overall actions reflect a violation of the law that not only caused financial loss, but also undermined the integrity of the banking system. The fact that IA used his authority to breach the bank's security procedures and systems indicates a very serious breach of professional ethics. Therefore, IA's actions are charged under various laws to ensure that justice is served and a deterrent effect is given, both to the perpetrators and to others who may intend to commit similar crimes.

Bank Jago, on the other hand, faces a major challenge in ensuring that customer confidence in the institution is maintained. As a financial institution, Bank Jago has a legal responsibility to protect its customers' funds and data. In this case, Bank Jago showed a proactive response by ensuring that no customer was financially harmed. The bank took steps to return the embezzled funds and enhanced their internal security systems to prevent similar incidents in the future. The fraud detection system that successfully identified this illegal activity is an important testament to the good implementation of anti-fraud principles in the bank's operations. However, this success is also a reminder that gaps in internal controls can be exploited by certain parties to commit crimes.

The steps taken by Bank Jago, such as the return of customer funds, improved security systems, and full cooperation with law enforcement officials, reflect the bank's commitment to legal and moral responsibility. However, this case still raises criticism of the bank's internal control system. For example, how was IA able to access the system to unblock accounts without being noticed for several months? Why is there no stricter oversight mechanism in place for the activities of employees who have access to sensitive data? These questions show that although Bank Jago has taken appropriate steps after the incident, there is a need to conduct a thorough audit of their supervisory system. From a legal perspective, this case provides important lessons on how existing laws are implemented to uphold justice in the banking sector. Legal action against the IA is not only aimed at punishing him, but also to provide a deterrent effect to other perpetrators who may intend to commit similar crimes. In addition, the steps taken by Bank Jago demonstrate the importance of institutional responsibility in addressing the impact of crimes that occur within its environment.

This case also provides a reflection for the banking industry as a whole. With the increasing complexity of modern banking systems that rely on high technology, the risk of cybercrime and misuse of system access is increasing. Therefore, financial institutions should continue to upgrade their security technology, while also providing training to employees on work ethics and the legal risks associated with abuse of authority. Existing regulations also need to be strengthened to include stricter oversight of internal banking activities.

Ultimately, this case emphasizes the importance of integrity in the management of the banking system. Not only should IA be held accountable for its actions, but Bank Jago as an

institution should also continue to demonstrate their commitment to improving security systems and internal controls. This case also provides valuable lessons for the banking industry on the importance of maintaining public trust through transparency, accountability, and strict application of the law against criminals. With these measures, it is hoped that public trust in the banking system can be maintained, while preventing the recurrence of similar cases in the future.

## CONCLUSION

The fraud case that occurred at Bank Jago, where a former employee embezzled IDR 1.3 billion in customer funds, revealed a number of weaknesses in the banking internal supervision system. The actions of the perpetrator, who took advantage of his authority to illegally unblock customer accounts and transfer funds to his personal account, not only violated professional ethics but also legal provisions, including the Information and Electronic Transactions Law (UU ITE), the Funds Transfer Law, and Law on the Prevention and Eradication of Money Laundering (UU TPPU). These findings show that the risk of misuse of access and weak internal controls are still major challenges for banking institutions in the digital era. Although Bank Jago succeeded in detecting suspicious activity through the early detection system implemented, the fact that the perpetrator was able to carry out his actions for several months without being detected indicates the need for a more comprehensive internal audit. Existing monitoring systems require improvement to ensure that the activities of employees with sensitive access are more closely monitored. In addition, this case highlights the importance of protecting customers' personal data in accordance with the provisions of the Personal Data Protection Law (UU PDP), which requires banks as personal data controllers to maintain security and ensure that there is no misuse of access by internal parties.

The application of advanced technology, such as artificial intelligence (AI) and big data analytics, is an urgent need to improve early detection of suspicious transaction patterns. This technology can help minimize the potential for fraud that is not detected by manual or conventional systems. In addition, ongoing training for employees is an important step to increase awareness about fraud risks, regulatory compliance and customer data protection. Stronger synergy between banking institutions and law enforcement officials is also needed to ensure the effectiveness of case handling and provide a deterrent effect for perpetrators.

This case is an important lesson for the entire banking sector to strengthen internal control systems, update relevant regulations, and implement the principles of good corporate governance. Bank Jago has taken corrective steps, such as returning lost customer funds and increasing the security of their system, but these steps must be followed by a thorough evaluation to prevent similar incidents in the future. Overall, the fraud case at Bank Jago emphasizes the importance of integrity in banking operations. Public trust in the financial system relies heavily on transparency, accountability and firm law enforcement. By strengthening the regulatory framework, implementing a comprehensive antifraud strategy, and building a work culture based on integrity, the Indonesian banking sector can create a safer and more sustainable financial environment.

**REFERENCES**


Djailani, Mohammad Fadil. 2024. "Bank Jago Dibobol Oknum Pegawai, Kepercayaan Nasabah Terancam?" *Suara.Com*. Retrieved December 12, 2024 (https://www.suara.com/bisnis/2024/07/16/144658/bank-jago-dibobol-oknum-pegawai-kepercayaan-nasabah-terancam).

Fadilah, Kurniawan. 2024. "Terbongkar Siasat Eks Pegawai Bank Jago Bobol Rekening Rp 1,3 Miliar." *Detiknews*. Retrieved December 12, 2024 (https://news.detik.com/berita/d-7433201/terbongkar-siasat-eks-pegawai-bank-jago-bobol-rekening-rp-1-3-miliar).

Mumpuni, Ayu. 2024. "Cara Mantan Karyawan Bank Jago Bobol Rekening Senilai Rp 1,3 M." *Tirto.Id*. Retrieved December 11, 2024 (https://tirto.id/cara-mantan-karyawan-bank-jago-bobol-rekening-senilai-rp13-m-g1u4).

Wanda, Alifin Nurahmana. 2020. "Pertanggungjawaban Tindak Pidana Perbankan Terkait Dengan Informasi Kerahasiaan Bank." *Indonesian Journal of Criminal Law* 2(1):1–14. doi: 10.31960/ijocl.v2i1.299.

Wicaksono, Adhi. 2024. "Bank Jago Buka Suara Terkait Eks Karyawan Bobol Rekening Nasabah." *CNN Indonesia*. Retrieved December 11, 2024 (https://www.cnnindonesia.com/ekonomi/20240710170329-78-1119762/bank-jago-buka-suara-terkait-eks-karyawan-bobol-rekening-nasabah).

Arifin, R. 2018. Law Enforcement In Banking Criminal Act Involving Insiders. *Jambe Law Journal*, *1*(1), 55–90. https://doi.org/10.22437/home.v1i1.7.

Efendi, J., & Rijadi, P. 2022. *Metode Penelitian Hukum Normatif dan Empiris: Edisi Kedua*. Prenada Media.

Kristanti, O., Kuntadi, C., & Pramukty, R. 2023. Faktor-Faktor Yang Mempengaruhi Efektivitas Sistem Pengendalian Internal: Peran Audit Internal, Karakteristik Auditor Internal, Dan Kualitas Audit Internal. *Sentri: Jurnal Riset Ilmiah*, *2*(8), 2899–2911. https://doi.org/10.55681/sentri.v2i8.1304.

Lestari, M. D., & Geraldina, I. 2023. Analisis Determinan Banking Fraud: Perspektif Crowe's Pentagon Fraud Theory (Studi Empiris pada Perusahaan Sektor Perbankan yang Terdaftar di BEI Tahun 2014-2018). *Jurnal Keuangan aan Perbankan*, *16*(2), 51. https://doi.org/10.35384/jkp.v16i2.312.

Muhammad, R. (2024). The Urgency of The Regulation of Legislative Power During The 'Lame Duck'Session to Optimize Constitutionalism. *Journal of Constitutional and Governance Studies*, *1*(1), 38-61.

Oktafian, I. 2024, July 11. Modus Pencurian Uang Nasabah Bank Jago, Pelaku Buka 112 Rekening yang Terblokir. *BeritaSatu.com*. Retrieved from https://www.beritasatu.com/dki-jakarta/2827987/modus-pencurian-uang-nasabah-bank-jago-pelaku-buka-112-rekening-yang-terblokir.

Daniel, et al. "Implikasi Hukum Terhadap Keamanan dan Perlindungan Nasabah atau Konsumen dalam Layanan Bank Digital." *ejournal.warunayama.org*, Nov. 2023, https://doi.org/10.3783/causa.v1i4.819.

Wicaksana, Dika Hikmah, et al. "Analisis Tinjauan Yuridis Terhadap Pembobolan Rekening Bank Digital Yang Dilakukan Pegawai Bank (Dalam Perspektif Hukum Perbankan Berdasarkan Studi Kasus Bank Jago 2023)." *Wicaksana | Media Hukum Indonesia (MHI)*, Nov. 2024, https://doi.org/10.5281/zenodo.14220517.

Surya Ningrum, Delvyan Putri. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia." *Journal Evidence of Law* 1, no. 1. 2022, https://doi.org/10.59066/jel.v1i1.472

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum, 6(1), 132-142. https://doi.org/10.38043/jah.v6i1.4484

Latumahina, RE, 2014, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya", Jurnal Gema Aktualia, Vol.3, No. 2, Hal. 14-25.